HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
APO AE 09128

DIRECTIVE
NUMBER 25-5

SECURITY

Information Assurance

---

1. Purpose. To establish an Information Assurance (IA) program for USEUCOM that integrates DoD policies and guidance, and supplements these to promote standardization and interoperability throughout USEUCOM.

2. Applicability. This directive applies to all USEUCOM elements to include HQ USEUCOM, USAREUR, USAFE, NAVEUR, MARFOREUR and SOCEUR, all USEUCOM-led JTF and CJTF, and other DoD elements operating in the USEUCOM Area of Responsibility. In addition, it applies to all other government organizations, government contractors and computer systems located within USEUCOM facilities.

a. Exemptions

(1) USEUCOM elements located within Department of State (DoS) facilities, or otherwise under the security cognizance of a DoS Regional Security Officer are exempted from this directive.

(2) Computer systems which are located within USEUCOM facilities, but which are neither owned nor operated by a USEUCOM element may be exempted from this directive. Exemptions shall be made by the appropriate Designated Approving Authority (DAA) on an individual case basis, giving consideration to the purpose of the system, the isolation of the system from other USEUCOM systems, and agreements with the system operator.

(3) Computer systems governed by policy that takes precedence over DoD Directive 5200.28 are exempted.

b. Conflicts with other DoD Directives. ED 25-5 implements DoD policy and guidance with minimal supplementation; therefore, conflicts with other DoD agency policy should be infrequent. Any conflicts that do arise shall be resolved on an individual case basis by the cognizant policy authorities.

3. Overview of the IA Program

a. The USEUCOM IA Program is based on DoD policy and guidance. The principal references are:

(1) DoD 5200.1-R, “Information Security Program” dated 14 Jan 97
(2) DoD Directive 5200.28, “Security Requirement for AIS” dated 21 Mar 88
(3) DoD Directive C5220.5, "Communications Security" dated 21 Apr 90
(4) CJCSI 6510.1B, “Defensive IO Implementation” dated 22 Aug 97
(5) CJCSI 6211.02A, “Defense Information System Network and Connected Systems” dated 22 May 96
(6) CJCSI 6470-01, “Military Telecommunications Agreement and Arrangements between the United States and Regional Defense Organizations”, dated 01 Sep 96
(7) ASDC3I Letter, “Secret and Below Interoperability (SABI)”, dated 20 Mar 97
(8) ASDC3I Letter, “Secret and Below (SABI) Reaffirmation”, dated 11 May 98

b. The USEUCOM IA Program interfaces with other related USEUCOM directives:

(1) ED 25-4, “Joint Key Management" dated 6 May 97
(2) ED 55-38, "Command and Control Warfare" dated 22 Sep 94 (under revision)
(3) ED 100-1, “Defensive Information Warfare” dated 10 Feb 97

c. This ED shall interface and adapt the above listed documents to USEUCOM operational requirements. The key points in the IA Program are:

(1) Minimum Security Requirements (to include training, security accreditation, network interconnections, intrusion detection, and technical requirements)

(2) COMSEC Monitoring

(3) Bulk Encryption Requirements

(4) INFOCONS

(5) IO Working Group

d. The appendices to this ED address specific IA subjects requiring special emphasis. Appendices shall be added, changed or deleted as DoD policy and guidance evolves, and as USEUCOM operational requirements change.

4. Proponent. The Chief, Defensive Information Warfare Division (ECJ6-I), HQ USEUCOM is the proponent for this directive. Address recommended changes and corrections to USEUCOM ISSM at DSN 430-8484: HQ USEUCOM, Attn: ECJ6-I, Unit 30400 Box 1000, APO AE 09128.

5. Theater Defensive Information Operations Working Group (IOWG). ECJ6-I shall chair the quarterly Theater Defensive IOWG consisting of representatives of EUCOM components and agencies (i.e., NCEUR, DISA-EUR). Responsible individuals are to take IA and DIO related issues to the Theater IOWG for resolution. The Theater IOWG shall appoint ad hoc working groups to address these issues as necessary.

a. The purpose of these ad hoc groups shall be:

(1) To facilitate sharing information
(2) To facilitate sharing resources
(3) To coordinate activities

b. Communications shall be primarily via e-mail, telephone and fax. Meetings shall be convened only as required. Business shall be conducted primarily on an informal basis.

6. Minimum Security Requirements. The following minimum requirements shall be met. Requirements which cannot be met shall be documented in the system accreditation documentation, SOP, operating plans or instructions or other documentation, and shall be resolved through the system's risk management program. Additional security recommendations are covered in Appendix C.

a. Training and Awareness. There shall be in place a security training and awareness program with training for the security needs of all persons accessing the AIS or communications system. The program shall ensure that all persons responsible for the AIS or communications system and/or information, therein, and all persons who access the AIS or communications system are aware of proper operational and security-related procedures and risks. Minimum requirements for security awareness training:

(1) The training shall be specific to the operational environment. Classroom training, video presentations, personalized instruction, and read-and-sign briefings are all acceptable methods of presentation.

(2) Each individual shall receive training prior to being granted access to any AIS or communications system and annual refresher training thereafter.

(3) Training records shall be maintained. At a minimum the records shall document that initial and annual refresher training was provided to each individual who has access to an AIS or communications system.

(4) All commands within USEUCOM shall have a training program for System Administrators following the format in Appendix A.

b. Accreditation. Command Designated Approval Authorities (DAA) are responsible for certification and accreditation of each system and network under their jurisdiction. Certification and accreditation shall be accomplished in accordance with DoD 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) dated 30 Dec 97 as well as guidance included in Appendix B.

c. Configuration Management. Commands shall implement a configuration management program for each system commensurate with the sensitivity, complexity, and mission criticality of the system. The programs shall control all system elements which enforce system security policy. Objective of the configuration management program is two-fold. Firstly, to provide a forum for evaluating the impact of proposed configuration changes on the system security profile. Secondly, to provide a forum for tracking and resolving risk management issues identified during system accreditation. Use of configuration management tools to establish and maintain a minimum security posture for networked systems (e.g., workstations, servers, mainframes, firewalls, routers, etc. and the software residing on them). To ensure the integrity of critical networked systems, distribution of hardware, firmware, and software must be under configuration management control and shall be provided an appropriate level-of-protection to assure product integrity. The use of standardized automation tools to establish and enforce configuration management is encouraged.

d. Network Interconnection

(1) Memorandum of Agreement (MOA). The interconnection of networks under the security cognizance of different DAA shall be documented in an MOA or similar agreement. See Annex B to Appendix B. The interconnection of networks under the cognizance of the same DAA should be documented in a security approval amending the security accreditation of each network.

(2) Firewalls. Networks that operate at the same security classification/compartmentation level, but with significantly different need-to-know requirements or other protection requirements, shall be interconnected using a firewall. The firewall shall be maintained under the physical control and system administration of the "high side" network.

(3) Security Guards. Networks that operate at different security classification/ compartmentation levels, to include U.S.-to-Allied networks, shall be interconnected using a security guard. Where a classified network is connected to an unclassified network, especially the NIPRNET/Internet, the guard shall be protected by a firewall, and monitored on both the high and low sides by an intrusion detection system (IDS). The guard, firewall and IDS shall be maintained under the physical control and system administration of the "high side" network.

(4) Multi-Level Security/Secret and Below Interoperability. All requirements to interconnect networks of different security classification/compartmentation levels, at the SECRET level or below, to include U.S.-to-Allied networks, shall be submitted to the MLS/SABI process for engineering review and security accreditation. The DAA for the networks are responsible for submitting the requirements through their command MLS/SABI POC to the NSA/DISA SABI team.

(5) Intrusion Detection Systems (IDS). All networks connected to the NIPRNET or INTERNET shall have an IDS. USEUCOM recommends (and the DSAWG may require) that a classified network connected to a network of lower security level employ IDS on both the "high" and "low" sides of the security guard that interconnects the networks.

NOTE: USEUCOM organizations have several classified networks which operate at hybrid security levels with foreign national users at the workstations (e.g., LOCE). The minimum security requirements for interconnection of these networks to any other network must be evaluated on an individual case basis. Refer questions to ECJ6-I.

e. Malicious Logic Protection. All AISs shall employ DISA-approved virus protection software obtained from a DoD-approved source. At a minimum, schedule anti-virus software to run on all networks and workstations daily, scan all incoming e-mail and file transfers for malicious logic/viruses before use, and establish procedures to rapidly obtain, distribute and install changes to anti-virus software on all information systems. Include virus prevention, detection, eradication, and reporting procedures in user awareness training. Viruses are a subset of malicious logic (e.g., virus, worm, Trojan horse, logic bomb, etc.) and current anti-virus tools are capable of detecting and eradicating most forms of malicious logic. USEUCOM authorizes and encourages the use of DISA approved virus protection software for home use as well.

f. Network Connection to Non-DoD and U.S. Activities. CJCSI 6211.02A, Defense Information System Network and Connected Systems, gives policy on the connection of the DISN and connected systems to non-DoD and non-U.S. activities. In addition to meeting the access and connection requirements for non-DoD U.S. activities, use of the DISN by foreign governments and allied organizations must be approved under the terms of CJCSI 6470.01, Military Telecommunications Agreement and Arrangements Between The United States and Regional Defense Organizations. Approved foreign users are subject to the same user agreement as DoD users. ASDC3I letter of 20 March 1997, Secret and Below Interoperability (SABI) and ASDC3I letter of 11 May 1998, Secret and Below (SABI) Reaffirmation policy require that interconnections between systems/networks at the SECRET level and systems/networks at lower levels (which includes any system/network with foreign national users), must be approved through the SABI process.

g. Audit Logs. AIS audit logs shall be maintained for a minimum of one year.

(1) DISA-EUR shall specify a minimum audit log data element set which shall enable correlation of AIS security incidents across multiple sites within the theater. This minimum data element set shall be implemented in all AISs. DAA’s may specify additional data collection requirements.

(2) All AIS audit logs shall have the capability to meet service requirements for legally admissible evidence.

(3) Audit log reduction and analysis should be migrated to a single, protected environment. The migration of audit log processing to a single, protected environment allows increased incident correlation across multiple AISs within a site and across multiple sites within the theater.

h. Encryption. All classified communications shall be secured using NSA-approved Type I encryption products, techniques and/or protected services. All FOUO communications shall also be secured using NSA-approved Type I encryption products, techniques and/or protected services whenever possible. Other sensitive but unclassified communications shall be secured using encryption products, techniques and/or protected services that have been evaluated by NSA or one of the NSA-approved evaluation laboratories. A specific risk determination must be made on using products that have not been formally approved by NSA, using NSA or laboratory evaluation results, the potential threat, and the level of sensitivity of the information being protected.

(1) There is no waiver to this policy for the transmission of classified information.

(2) Sensitive information as defined in the Computer Security Act of 1987 and Sensitive But Unclassified (SBU) information shall not be posted on nor transmitted over the Internet/NIPRNET without appropriate NSA-approved products, techniques and/or protected services, or those that have been evaluated by NSA or an NSA-approved evaluation laboratory as being suitable for protections of sensitive information. Temporary waivers can be granted on a case-by-case basis for systems that do not currently have an encryption capability for Sensitive and SBU information. For systems where no encryption means is currently available, managers responsible for the system are required to inform all users of the danger of passing Sensitive and SBU data over that system, and are further responsible for notifying ECJ6-I of the lack of encryption capability and the steps being taken to provide such capability.

i. Bulk Encryption. All USEUCOM links/trunks shall be bulk encrypted. Appendix F contains a more detailed description of USEUCOM's Bulk Encryption policy and a sample waiver request form.

j. COMSEC Monitoring. Communications Security (COMSEC) monitoring or Operational Force Protection Communications Support is required for all USEUCOM and USEUCOM-directed JTF operations. Requests should be submitted to ECJ6-I for tasking to the Joint COMSEC Monitoring Activity (JCMA). COMSEC monitoring should also be requested for all exercises which are USEUCOM directed or led by a USEUCOM-directed JTF.

(1) Components shall certify to ECJ6-I their compliance with DoD Directive 4640.6 notification and consent requirements biannually in even numbered years, running from 1 October of the current even numbered year to 30 September two years following.

(2) The purpose of COMSEC monitoring is to determine the amount of protection being provided to classified or sensitive information in order to provide a measure of force protection to the commander. Results of COMSEC monitoring should be shared among involved components and USEUCOM Headquarters to the maximum extent possible, in order to share lessons learned and improve the theater COMSEC posture. JCMA shall be authorized to share any information

that is life- or mission-threatening with other components or commands affected by the information revealed, when they are operating under HQ USEUCOM, component or JTF/CTF tasking.

k. MLS/SABI. All Multi-Level Security (MLS) interconnections or requirements for interconnections between two networks of different security levels, or between any U.S. and any non-U.S. network shall be identified to ECJ6-I. For interconnections between systems at the SECRET level or below, the cognizant DAA is further responsible for submitting the interconnection requirement to the SABI (SECRET and Below Interoperability) process.

7. INFOCONS. USEUCOM shall direct changes to theater Information Operations Conditions (INFOCONS) as required by the combination of threats, vulnerabilities, political and military conditions, and friendly operations. USEUCOM may direct specific measures to be taken with a change in INFOCON, or may direct that all applicable INFOCON level measures be taken. Components may declare a higher INFOCON level for their own component elements, and may enact additional measures, but any such changes or additions must be reported to the USEUCOM IO Cell (as described in ED 100-1) immediately for purposes of informing lateral elements and the Joint Staff. Specific reporting requirements for achievement of directed measures shall be provided in the message declaring an INFOCONS change. INFOCONS measures are published in Appendix D.

8. IAVA. Information Assurance Vulnerability Alerts (IAVA) are directed by the Joint Staff and transmitted through DISA. USEUCOM activities shall utilize the Incident Reporting Process defined in Appendix D, Annex B of this Directive to acknowledge IAVA receipt and report accomplishment of directed actions. Components shall acknowledge IAVA receipt and report accomplishment of directed actions through their service channels with information copy to DISA-EUR.

9. Release of COMSEC Equipment to Foreign Allies. All USEUCOM components and elements must follow the procedures listed in Appendix E to this Directive whenever they determine there is a requirement for releasing COMSEC information or equipment to a foreign government. This Appendix implements procedures to meet the requirements of CJCSI 6510.01B.

FOR THE COMMANDER IN CHIEF:

OFFICIAL:

MICHAEL A. CANAVAN
Lieutenant General, USA
Chief of Staff

SUSAN M. MEYER
LTC, USA
Adjutant General

APPENDICES
See Table of Contents

DISRIBUTION:
P

(This page intentionally left blank)

APPENDIX A – PROGRAM MANAGEMENT

1. Information System Management Structure. The following Information System Security positions have been identified for USEUCOM: Designated Approving Authority (DAA), Information System Security Manager (ISSM); Information System Security Officer (ISSO); and System Administrator (SA).

a. Each Information System Security position shall be designated in a formal duty appointment which specifies all duties and responsibilities, including the facilities, organizational elements, or computer systems for which the appointed person is responsible.

b. All persons appointed to one of these Information System Security positions shall receive training in the proper execution of their job and Information Assurance responsibilities prior to commencing their new responsibilities

c. Commands are encouraged to adopt the term ISSM, ISSO, and System Administrator except when it conflicts with other directives, or when adoption of the term would be cost prohibitive or lead to confusion. Commands should define other supporting positions (i.e., Remote Terminal Area Security Officer, ISSO Agent, Work Group Administrator).

2. Designated Approving Authority (DAA). The DAA is the official responsible for authorizing the operation of an information system once based on evaluation of risk. If the level of risk is deemed acceptable, the DAA is responsible for issuing an accreditation statement. The accreditation statement indicates that the DAA formally accepts security responsibility for the operation of the system and officially declares that the specified system is adequately protected against compromise, destruction, or unauthorized modification under stated parameters of the accreditation. The Designated Approving Authority (DAA) has the overall responsibility for the secure operation of the information system; makes appropriate decisions to balance security requirements, mission, and resources against the defined or perceived threat; and ensures resources are expended to support the certification and security countermeasures process. The DAA shall:

a. Review and approve security safeguards, ensure that each information system is properly accredited based on its environment and sensitivity levels, and issue written accreditation statements.

b. Ensure an effective information system security education, training, and awareness program is in place.

c. Ensure that data ownership is established for each information system, to include accountability, access rights, and special handling requirements.

d. Take action, where the certification authority has recommended a denial to accredit, to achieve an acceptable security level (e.g., allocate additional resources).

e. Appoint an Information System Security Manager (ISSM), Information System Security Officers (ISSO) and Network Security Officer (NSO).

3. Information System Security Manager (ISSM). The command's ISSM serves as the single point of contact for Information System Security program management and all command-level Information System Security issues. Information System Security program management includes promulgating Information System Security guidance within the command, developing command-unique policy, establishing an Information System Security training program, and insuring that each system is properly accredited and has an appointed ISSO. Command designated ISSMs supervise and coordinate the activities of ISSOs within a specified facility or organizational element and could perform selected ISSO duties and responsibilities. In addition, the primary ISSM should serve as the command DAA's staff officer for evaluating security accreditation.

4. Information System Security Officer (ISSO). An ISSO shall be appointed for each computer system, grouping of computer systems, computer network, or grouping of computer networks. The duties and responsibilities of an ISSO are specified in paragraph E.9.d of DoD Directive 5200.28. For additional guidance on the duties of an ISSO see NCSC-TG-027.

5. System Administrator (SA). Services and agencies have various definitions of system administrator, but in all cases systems administrators are generalists. They install, tune, and maintain information systems and associated networks.

a. System Administrators typically perform the following duties:

(1) Install and configure software and subsequent security patches
(2) Teach users operational duties and solve operations-related problems
(3) Write scripts/programs
(4) Repair or upgrade hardware,
(5) Help enforce security

b. It is the System Administrator who keeps an information system environment up and running for their users. The correct implementation and configuration of system security mechanisms is the responsibility of the System Administrator. The System Administrator is also the first person to whom the user should turn when noticing a problem with the system or security.

APPENDIX A – PROGRAM MANAGEMENT

Annex A – System Administration

1. System Administrator Training and Licensing. All commands shall implement a System Administrator Training and Licensing Program. System Administrators install, tune, and maintain information systems and associated networks. Along with Information System Security Officers, system administrators enforce security.

2. System Administrator Levels. The level is used for its simplicity and relation to skill levels used by the uniformed services. The breakdown of levels and tasks does not take into account the practice of specialization. The requirements outlined at each level are subjective. Level recognition can be loosely based on an individual's status with existing information system career panel organizations. The term domain is used as a way to bound the focus, or realm of control, of any given information system management organization, regardless of size. (The time lines described are for general guidance, not directive.)

a. Level #1. System Administrator is a novice with limited operational experience. Individuals reach Level #1 status after a predetermined time of on-the-job training, usually no sooner than one year on the job.

Skills. Recommend at least one year of experience administering the relevant operating system; formal training for the operating system and command language, strong customer service skills.

Tasks. Day-to-day operations such as backups, restores, adding / modifying / deleting user accounts; installing operating systems, applications, and peripherals; troubleshooting user problems; debugging command language scripts; assisting the ISSO in access control security.

b. Level #2: These are the workhorses in a domain. They perform the majority of the daily tasks that keep a domain running smoothly. They are expert technicians that can work simultaneously on several problems. At least half of the System Administrators in a healthy domain should be at Level #2.

Skills. Recommend at least three years of experience in administering the relevant operating system; formal training in networking, programming language concepts and algorithms; formal training in firewall management and telecommunications fundamentals; knowledge of all interactions within their domain; ability to program in a command language; ability to spot redundant tasks and automate them; strong communications skills; independently resolving non-trivial problems; working in groups to jointly solve problems; with the ISSO, ability to successfully implement security mechanisms on networks and systems within their domain; serve as an informal mentor to Level #1 System Administrators

Tasks. Taking lead in solving day-to-day problems; implementing complex system changes; ensuring that established security mechanisms are functioning properly; debugging operating system, application, and network problems; following domain parameters, defining default environment for systems for users; maintain and enforce adherence to standards; monitor and balance load among servers and networks within domain; interacting with developers, operations centers, and support personnel to maintain daily operations; keeping the environment up and running smoothly.

c. Level #3. The truly experienced administrators. Large domains should have one or two Level #3 administrators leading the technical effort and setting the policy and direction for the domain. The absence of a Level #3 tends to leave the domain with no clear direction

Skills. Recommend at least five years or more extensive experience; formal training covering at least: operating system design, date / Algorithm structure, machine architecture, networking, programming language concepts / algorithms; strategic view of the domain operation and interaction with external domains; fluency in at least one command language; experience with applicable programming languages; ability to work independently; ability to lead a team to quickly and completely solve problems; strong interpersonal, organizational, and communications skills; ability to train junior system administrators.

Tasks. Taking general direction; setting standards; planning and designing the architecture of their domain; working with the ISSM and ISSO, planning security procedures, mechanisms, and architecture of their domain; tuning the performance; solving the tough problems; leading teams to tackle complex problems; teaching; publishing guidance and lessons learned.

APPENDIX B – ACCREDITATION

1. All systems that process classified information or sensitive unclassified information (e.g., FOUO, Privacy Act Data) must meet the applicable security requirements and be formally accredited by the cognizant DAA.

2. DAAs shall maintain a valid accreditation for all systems deployed to and operated in the USEUCOM AOR throughout their operational life cycles. 'System' for the purposes of this appendix is defined as the combination of new software applications and hardware.

3. USEUCOM strongly recommends against using live operational networks, especially those connected to the DISN, to support demonstration or testbed systems. In any case, the cognizant DAA for the supporting system must grant security approval to operate the demonstration or testbed system.

4. Effective as of the date of this ED, systems operating under an Interim Approval To Operate pending a final accreditation decision are not required to change accreditation methodology and documentation to conform to the DITSCAP standard.

5. DAAs shall have a risk management program for each system under their control. Risk management programs shall be documented in an appendix to the System Security Authorization Agreement. The appendix shall contain, as a minimum, the following information on each vulnerability identified throughout the system cycle:

a. Description of vulnerability (including date/time discovered)

b. Potential system/mission impact if not resolved

c. Date entered into configuration control process

d. Date resolved

(This page intentionally left blank)

APPENDIX B – ACCREDITATION

Annex A – System and Network Interconnections

1. Memorandum of Agreement (MOA)

a. When AISs managed by different DAAs are interfaced or networked, an MOA is required that addresses the accreditation requirements for each AIS involved. A sample MOA is included in Annex B to Appendix B. In addition to meeting the requirements established in DoD 5200.28, the MOA shall include:

(1) Key security aspects of the two systems which affect their interconnection and interoperation.

(2) Description of the interconnection and outline of the responsibilities, procedures and agreements for operating the interconnection.

(3) Risk assessment of the interconnection which focuses on risks which arise or change resulting from the interconnection.

b. An MOA is not required when two systems interface via the SIPRNet. Interconnection risk identification and mitigation requirements are met through the DISN Connection Approval Process.

c. An MOA is not required when two systems interface via the NIPRNet. It is not realistic to expect commands to implement a process similar to the DISN Connection Approval Process even though the risk of interconnecting systems via the NIPRNet warrants additional analysis.

d. An MOA is required for all other cases of system or network interconnection.

e. DAAs shall coordinate configuration changes which impact the security posture documented and agreed to in an MOA prior to making the change.

2. DISN Connections

a. All commands desiring connections to DISN resources shall maintain an up to date Authority to Connect (ATC) or Interim Authority to Connect (IATC) via the DISN Connection Approval Process. USEUCOM shall not support continued connection to DISN resources for networks which have expired ATCs or IATCs.

b. All vulnerabilities identified during the Connection Approval Process and subsequent DISN vulnerability assessments shall be corrected. Commands shall notify ECJ3 and ECJ6 in the event correction of a vulnerability has a mission impact and a work-around is not available or is cost-prohibitive.

(This page intentionally left blank)

APPENDIX B – ACCREDITATION

Annex B – Sample Memorandum of Agreement

The following is provided for informational purposes only. Commands may adopt this format, edit it to suit their needs, or create their own format.

[Notes and Instructions to the Preparer, Version 980914]

1. or the purpose of this MOA, "system" is defined as any computer system, computer network, or communication system used to interconnect computer systems.

2. Replace System1 and System2 throughout this document with actual system names.

3. Notes and instructions for completing this document are enclosed in [ ] throughout the document. Remove all notes and instructions from the final copy submitted for signature.

4. Include in Annex A all POCs that are identified in the MOA.

5. Use this document as a template, adapting it where necessary to fit the interconnection. Do not blindly copy the text.

6. Reminder: Interconnections with systems operated by non-DoD and non-U.S. elements must comply with CJCSI 6740.01 "Military Telecommunications Agreements Between the U.S. and Regional Defense Organizations" and CJCSI 6211.02 "DISN and Connected Systems".

7. Reminder: Agreements with non-DoD and non-U.S. elements must be submitted to the Command Legal Advisor for legal review.]

Memorandum of Agreement
for Interconnecting
System1
and
System2

This Memorandum of Agreement (MOA) establishes the security responsibilities and procedures for interconnecting System1 and System2. This MOA is between the Designated Approving Authority for System1 and the Designated Approving Authority for System2.

1. Assertions About System1 and System2. The purpose of this section is to outline the key security aspects of the two systems which affect their interconnection and interoperation.

a. System1.

(1) The Security Level and Security Mode is:

[Note: Include any special categories of information that require formal security accesses, and any dissemination controls which define the security level of the system.]

(2) The minimum required security clearance level of users is:

(3) Foreign nationals do not have user or keyboard access to the system, nor do they have unescorted physical access to the network components. [If this assertion is not correct, replace it with an appropriate assertion.]

(4) Identification and Authentication

(a) The system forces all personnel with user or keyboard access to complete an identification and authentication process prior to gaining access to system resources.

[If this assertion is not correct, replace it with an appropriate assertion.]

(b) Each person who is authorized to access the system is identified to the system as a unique user (vice as a group or team). [If this assertion is not correct, replace it with an appropriate assertion.]

(5) DoD Logon Warning Banner

(a) A DoD Logon Warning Banner is displayed to each user at each session logon. [If this assertion is not correct, replace it with an appropriate assertion.]

(b) The user must acknowledge the DoD Logon Warning Banner prior to gaining access to any system resources. [If this assertion is not correct, replace it with an appropriate assertion.]

(6) Audit Logs

(a) The system audit logs capture all system-level access events (e.g. user logons, logoffs, failed attempts) and use of critical system functions. [If this assertion is not correct, replace it with an appropriate assertion.]

(b) The system audit logs and all supporting records are retained for at least [insert the period of time, such as 30 days, six months, three years].

(7) The system is not connected to any other system of lower security level or which has foreign national users. [If the assertion is not correct, replace it with an appropriate assertion.]

(8) Points of Contact for the system are listed in Annex A. The [insert position title such as ISSO] is responsible for keeping the System1 section of this Annex current, and providing the System2 counterpart with revisions.

(9) Letter of Accreditation (or Interim Authority to Operate) is enclosed at Annex B. The [insert position title, such as ISSO] is responsible for keeping the System1 section of this Annex current, and providing the System2 counterpart with all updates.

(10) The primary security directives, regulations and instructions governing operations and interconnection with other systems are:

(11) Other Assertions [If none, delete this entry.]

b. System2. [Provide assertions for System2 using the same format as for System1.]

2. Description and Operation of the Interconnection. The purpose of this section is to describe the interconnection, and outline the responsibilities, procedures and agreements for operating the interconnection.

a. Attached at Annex C is a network connectivity diagram that clearly identifies the system interconnection point, all System1 and System2 devices which directly connect to or support the interconnection, the IP addresses of the interconnecting devices, and the IP address ranges of System1 and System2. Also attached at Annex C is a high-level connectivity diagram of System1 and System2 showing key network devices and interconnections with other systems.

b. The demarcation point which separates System1 from System2 is:

c. The interconnection [does/does not] include a device that is shared by System1 and System2. [Edit the remainder of this paragraph as required.] Offices that are responsible for this device are listed below.

(1) Designated Approving Authority

(2) System Operational Authority

(3) Configuration Management

(4) System Administration

(5) Information System Security Officer (ISSO)

(6) COMSEC keying material

(7) Initial Installation of the Device

(8) Hardware Maintenance

d. Physical Location

(1) The system interconnection is physically located in: [enter room number, building number, name of facility, city and country; or enter appropriate answer for mobile facilities and field operations.]

(2) Security level to which the interconnection room is protected.

(3) Categories of personnel who have unescorted access to the interconnection room: [e.g., System2 system administrators only; anyone with facility access and appropriate security clearance].

e. Information Flow

(1) Types of data or services (e.g., protocols, network services, IP addresses) that shall be and shall not be allowed to pass between the systems.

(2) Devices that shall be used to implement these controls, and the offices responsible for administration of these devices.

(3) Procedures for administering information flow controls:

(4) Information flow across the interconnection [shall/shall not] be audited [as follows:].

f. Security Incident Reporting. All security incidents involving the system interconnection shall be reported as soon as possible to the Security Incident POCs noted in Annex A. Critical incidents (e.g., compromise of classified information; denial-of-service attack directed against any of the interconnected systems) shall be reported immediately. If the designated POC cannot be contacted, the incident shall be reported to the 24-hour, 7-day POCs noted in Annex A. [If the assertion is not correct, replace it with an appropriate assertion.]

g. On-Line Vulnerability Assessments (VA). On-Line VA includes "penetration testing" and executing any "security tools" to determine the security profile of a system. [If the following assertions are not correct, replace them with appropriate assertions.]

(1) System managers may conduct VA on their own respective systems up to the demarcation point without restriction, notification or approval of the system managers of the system beyond the demarcation point.

(2) System managers shall not conduct a VA on the shared interconnection device without prior approval of the [insert position title such as ISSO] for System1 and the [insert position title] for System2.

(3) System managers shall not conduct VA that includes any part of the system beyond the demarcation point without prior approval of the DAA for that system.

3. Risk Assessment. The purpose of this section is to focus on the risks which arise or change because of the interconnection. Attached at Annex D is a risk assessment which identifies all significant risks to either System1 or System2 that shall result from this interconnection.

4. Execution

a. This MOA becomes effective on the date of the last signature of the parties listed below and shall remain in force until terminated by any party listed below.

b. This MOA may be terminated at any time by mutual consent. Either party may terminate it by serving written notice to the other party 90 days prior to the termination date.

c. Minor Changes to the MOA. The categories of minor changes outlined below can be made to this MOA without the approval of the signatories. Minor changes are those which do not constitute a significant change to the nature or purpose of the interconnection, and which do not have a significant impact on the overall risk assessment of the interconnection. [For each category of authorized minor change, identify the persons authorized to make the change and procedures for formalizing the change. Example: adding the IP address of an additional web server to a list of authorized web server addresses in a filtering router can be approved by agreement between the SA for each system via e-mails, which shall be added to the Information Flow section as an amendment.] [If minor changes are not authorized, enter "Not Authorized" after the paragraph header.]

d. Major Changes to the MOA. Each party is obligated to notify the other party of major changes to their respective systems, when these could affect the interconnection. Major changes are those which constitute a significant change to the nature or purpose of the interconnection, or which have a significant impact on the overall risk assessment of the interconnection. Major changes may require executing a new MOA, amending the MOA or terminating the MOA. [Examples: change to accreditation parameters of a system; adding a direct connection from a classified system to the Internet; adding web browsing capability to an interface which was previously restricted to e-mail only.]

e. Conflicts that cannot be resolved at the operational level shall be resolved by [insert name of DAA]. This DAA shall have the authority to disconnect any system or device that is not in compliance with the terms of this agreement.

f. This MOA shall be reviewed at least yearly to ensure it remains current.

5. Signature Blocks for Designated Approving Authorities. We have reviewed the Memorandum of Agreement (MOA) for the interconnection of System1 and System2. We have determined that the terms for operating this interconnection, and the increase in risk resulting from the

interconnection is acceptable. This MOA is hereby approved, and the interconnection may be established.

	System 1	*System 2*
Name		
Title		
Organization		
Signature		
Date		

MOA Annex A
Points of Contact

1. System1

   a. Information Systems Security Officer (ISSO)

      (1) Name:
      (2) Organization:
      (3) Phone:
      (4) Fax:
      (5) E-mail:

   b. System Operational Authority

      (1) Name:
      (2) Organization:
      (3) Phone:
      (4) Fax:
      (5) E-mail:

   c. System Administrator

      (1) Name:
      (2) Organization:
      (3) Phone:
      (4) Fax:
      (5) E-mail:

   d. Security Incident Reports

      (1) Name:
      (2) Organization:
      (3) Phone:
      (4) Fax:
      (5) E-mail:

   e. 24-hour, 7-day POC for all matters (e.g., Help Desk)

      (1) Organization:
      (2) Phone:
      (3) Fax:
      (4) E-mail:

2. System2. [Provide information for System2 using same format as for System1].

3. Shared Interconnection Device. [If applicable, provide information using same format as for System1.]

MOA Annex B
Letters of Accreditation (or IATO)

Attached to this Annex are the current Letters of Accreditation or Interim Approvals to Operate for System1 and System2.

MOA Annex C
Network Connectivity Diagrams

Attached to this Annex is a network connectivity diagram which shows the IP address ranges for System1 and System2 and the IPs of the devices involved in the physical interconnection.

Annex D
Risk Assessment of the Interconnection

This risk assessment of the interconnection focuses on significant risks which arise or change because of the interconnection.

----------Notes and Instructions to the Preparer----------

1. For each risk, identify:

   a. What is at risk?
   b. Why is it at risk?
   c. What is the likelihood of occurrence?
   d. What is the likely impact?
   e. What practical measures could be implemented to reduce the risk?

2. Listed below for your information only are common threats and vulnerabilities that can arise because of interconnections.

   a. <u>Threats</u>

      (1) Increase in combined user population increases the threat of insider attack to each system.

      (2) Existing threat to one system becomes a threat to the other system.

b. Vulnerabilities

(1) The resulting combined (interconnected) system is more complex, therefore more vulnerable to internal and external threats.

(2) Existing vulnerability to one system becomes a vulnerability to the other system.

(3) If a new interdependency of one or both systems arises because of the interconnection, then one or both systems are now more vulnerable to any attack on the supporting system or on the interconnection devices. Examples: elimination of redundant system components, elimination of redundant connections to backbone networks.

(4) Lack of authority of system officials to conduct unannounced physical inspections of the other system, or to conduct on-line vulnerability assessment on the other system.

(5) Unknown backside connections to the other systems.

(6) Lack of trained personnel or sufficient personnel to properly install and maintain interconnection devices.

(7) Inability to reconcile audit logs from the two systems, or to trace user access across the interconnection impacts the ability to resolve security incidents.

(This page intentionally left blank)

APPENDIX C – ADDITIONAL SECURITY OPTIONS

Commands shall implement security requirements at the command level to promote security standardization and interoperability throughout USEUCOM in accordance with DoD policy and as supplemented in this appendix.

1. Internet Connection. (Component commands shall follow service policies on authorized use of the Internet. An NSA evaluated device to control access to a network must be installed at the enclave boundary to the NIPRNET. This connection component may be a firewall-type device or filtering router.) Prior to transmitting any information over a publicly accessible network (e.g., NIPRNET, INTERNET), or storing any information on a publicly accessible computer system (e.g., a server connected to the NIPRNET), consideration shall be given to the releasability of the information to the general public or to the criticality of the information. These factors may:

a. Warrant the use of additional security measures such as writer-to-reader encryption, FORTEZZA cards, integrity checks or firewalls; or require prior clearance from a command Public Affairs Office, especially if the information shall be placed on a World Wide Web server. Procedures for clearing electronic copies of information should be in consonance with procedures already in place for clearing "hard" copy information.

b. Be consistent with other leadership responsibilities for public and internal communication, the decision whether or not to establish an organizational web information service is delegated to the local commander. The local commander may delegate this authority to lower levels, but shall ensure that all information placed on publicly accessible web information services is properly cleared and released. Local commanders or their designee shall ensure that appropriate instructions and regulations governing the clearance and release of information on web information services are published.

c. Information on the Internet. No information on the World Wide Web or Internet shall be posted that compromises national security or place USEUCOM personnel at risk. This prohibition includes information that is sensitive, CLASSIFIED, and privacy act protected.

d. Self Executing Programs or Applets. Features such as ActiveX and Java applets have the capability to install malicious programs on network computers. The same danger exists when downloading executable files. ActiveX and Java features should be disabled (browser security default setting) and only activated by exception when accessing trusted web sites.

2. Network Connection by Foreign Nationals. Ref (aa) gives policy on the connection of non-DoD U.S. government entities and foreign nationals. In addition to meeting the access and connection requirements for non-DoD U.S. activities, use of the DISN by foreign governments and allied organizations must be approved under the terms of ref (bb). Approved foreign users are subject to the same user agreement as DoD users. Security devices providing foreign connections to the SIPRNET must be approved through the SABI process.

3. Maintenance. Maintenance on computers used for processing classified data should be performed by personnel who are cleared for the most sensitive data processed by the system. Foreign national personnel shall not perform maintenance on computers used for processing classified data, unless specifically authorized by the DAA. If the maintenance personnel are not cleared for the most sensitive data processed, then:

a. The computer shall be declassified prior to maintenance, per the sections of this document dealing with remanence and disposal, or

b. The maintenance personnel shall work under continuous supervision of cleared personnel who are knowledgeable of the system operations and who are able to control the access to information in the system.

4. Music CDs. CD technology is rapidly evolving. CD-EXTRA, multimedia CDs containing music, video, text, and executable object code are now on the market. The packaging of these CD-EXTRA discs does not always alert the purchaser that this is a CD-EXTRA formatted disc. If the CD-ROM player attached to a PC has the ability to recognize the CD-EXTRA format, the executable on the disc can automatically execute. The executable can be valid object code or malicious code, e.g., viruses, Trojan Horses, etc. Commands should develop a policy for the use of music CDs in DoD computers. If music CDs are to be allowed, PCs should be configured to disable the autoplay feature, and CDs must be virus checked prior to use.

5. Desktop video teleconferencing. Be wary of cameras and microphones that can be remotely panned and zoomed. Use them only where required, and put them in an area where no sensitive information would be disclosed by their accidental or deliberate misuse. If computers include microphones and/or cameras capabilities that are not being used, they should be disconnected or physically disabled.

6. Toner Cartridges. Drum type toner cartridges commonly used in standard laserjet printers have the potential of retaining data on the cylinder heads after use. It is recommended that five pages with no margins of random alphanumeric characters be printed (prior to disposal of a cartridge used on a classified system).

7. User Logins

a. If a userid and password control access to an account on a system processing marked and protected information, then the userid and password combination is classified at the highest level encountered on that system (e.g. US SECRET NOFORN if the system processes up to U.S. SECRET NOFORN). Handling requirements for classified userid and password combinations are the same as for any other information of the same classification level.

b. If a userid and password control access to an account on a system which processes unclassified information, the userid and passwords are considered Sensitive Information as defined by the Computer Security Act of 1987. As such, they must be protected during the login process with appropriate NSA-endorsed products, techniques and/or protected services.

Temporary waivers can be granted on a case-by-case basis for systems that do not currently have an encryption capability for Sensitive information. For systems where no encryption means is currently available, managers responsible for the system are required to inform all users of the danger of logging into that system, and are further responsible for notifying ECJ6-I of the lack of encryption capability and the steps being taken to provide such capability.

8. Remote Access via Modem. Remote access must be provided with an appropriate level of authentication, encryption and physical protection to match the classification of the accessed information system. Access tables must remain current. Prohibit the use of call-forwarding capabilities when callback or dialback technology is used. Annotate remote access in the audit logs. Employ methods for controlling access (e.g., callback, token generation, etc.), where the capability exists.

9. Software patches. Install vendor-produced system patches and implement procedural countermeasures according to DISA-EUR or ASSIST guidance immediately upon receipt. In the rare case where security relevant system patches cannot be implemented, exceptions must be approved by the DAA and documented in the risk analysis. Forward copies of the approved exceptions and updated risk analysis to DISA-EUR and ECJ6-I.

(This page intentionally left blank)

APPENDIX C – ADDITIONAL SECURITY OPTIONS

Annex A - Marking

1. Executive Order 12958 (ref z) "prescribes a uniform system for classifying, safeguarding, and declassifying national security information." It requires that classified documents "shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification...and which portions are unclassified." Complying with the requirements of ref (z), shall require the labeling of information residing in electronic classified information systems. At a minimum, all electronic classified information in the form of documents, images, or other human-viewable format shall require plain-text markings indicating classification, handling restrictions, classifying authority, and declassification instructions, as would be required if they were paper products. New databases or other similar data repositories should include database columns for the identifying plain-text labels, or equivalent methods for labeling data elements.

a. System Identification Screen. All computer display monitors shall display a system identification screen prior to allowing any logon. This screen shall include the following information:

(1) The security classification level of the system, essential control markings and compartments (e.g., UNCLASSIFIED, SECRET REL NATO, TOP SECRET SI/TK). This requirement is optional for unclassified systems and networks that are not intended for use in an area where classified information is processed.

(2) The name of the proponent organization for the system or network (e.g., HQ U.S. European Command; U.S. Army 5th Signal Command). The name may be displayed within an organizational logo, if the name is compete and legible.

(3) The name of the system or network (e.g., Global Command and Control System; HQ USEUCOM SECRET LAN)

(4) The DoD Logon Warning Banner. All AIS shall display a DoD-approved logon warning banner. Service commands may use a warning banner approved by their service. The banner shall be included in the system identification screen. If the banner shall not fit in this screen, it shall be displayed in an alternative manner as prescribed by DoD policy or service policy. Personnel shall not be permitted to log in without agreeing to the login banner.

b. Softcopy documents

(1) These documents include, but are not limited to: e-mail, memos, charts, and web pages/files. This includes documents in any state of completion, including official and draft documents.

(2) Minimum requirements within USEUCOM shall include individual paragraph or portion makings; classification at top and bottom of pages or at top and bottom of web file, and "Derived by / declassify on" markings on all softcopy documents.

(3) All markings shall allow a user to quickly and continuously be aware of the classification of the document / web page or file.

(4) All information to be published on a web page must be reviewed with the "Need-to-Release" principle in mind. Carefully consider whether the information should be made widely available.

(5) All web pages should be classified based on their individual content, regardless of the classification of the pages to which it links.

c. E-mail. It is suggested that each command adopt a common methodology for quickly identifying the classification of e-mail. At HQ USEUCOM, for example, the subject line starts with the classification of the e-mail, followed by the subject, and ends with the classification of the subject line. All e-mail will begin with a banner stating the classification of the e-mail. Unclassified e-mail with classified attachments marked as classified, are marked with a second banner stating "UNCLASSIFIED WHEN CLASSIFIED ATTACHMENTS REMOVED". Classified e-mail with classified attachments also contains a second banner when the classification of the e-mail is lesser than the classification of the attachment, for example "DOWNGRADE TO CONFIDENTIAL WHEN UNCLASSIFIED ATTACHMENTS REMOVED". Further guidance on how to apply markings can be found in DoD 5200.1-PH.

APPENDIX C – ADDITIONAL SECURITY OPTIONS

Annex B – Remanence/Media Reuse

1. Data *remanence* is the residual physical representation of data that has been erased from storage media. After storage media is erased there may be some physical characteristics that allow data to be reconstructed. There are two means of destroying data on magnetic media: overwriting and degaussing.

a. *Overwriting* destroys data on storage media by recording patterns of unclassified data over the data stored on the media. There are several means by which old data can remain on an overwritten hard drive. Blocks that are marked "bad" are not overwritten when a drive is reformatted. The overwrite program may fail to locate and overwrite every area of the drive. The drive may have several partitions, and the user and overwrite procedure may only be aware of one of them. Finally, errors and drift in the hard disk's tracking signal may leave enough of the old data signal behind for a lab to recover the overwritten data.

b. *Degaussing* (also known as demagnetizing) reduces magnetic induction to zero by applying a reverse magnetizing field. Unfortunately degaussing erases the hard drive's tracking signal along with the data signal, essentially destroying the drive (unless the manufacturer can record a new tracking signal on the drive). As data densities on hard drives increase, so do the coercivities of their magnetic media, requiring stronger and stronger degaussing equipment.

2. The Department of Defense requires the use of DoD 5200.28-M by DoD components, but heads of DoD components may augment these requirements to meet their needs by prescribing more detailed guidelines and instructions provided they are consistent with these policies. Ultimately, the Information Systems Security Manager (ISSM) is responsible for the security of all ISs and media assigned to the organization and under their purview. To protect these assets, ISSMs must ensure that the applicable DoD and service security measures and policies are followed.

3. Users wishing to downgrade, declassify or release media are to contact their governing ISSO, who shall make decisions and prescribe procedures based on the applicable DoD and service regulations.

4. Equipment Disposal. Commands shall insure that computer systems and computer storage media which have been used for processing classified information or sensitive unclassified information are appropriately erased, declassified or destroyed prior to transfer to a DoD supply system, the DRMO, an entity outside DoD, or trash bins. Commands should follow their service guidelines for sanitizing and releasing equipment. It is recommended that no previously classified magnetic media be disposed of via DRMO.

(This page intentionally left blank)

APPENDIX C – ADDITIONAL SECURITY OPTIONS

Annex C – Removable Hard Drives and Periods Processing

1. Commands are encouraged to adopt a policy requiring all computer hard disk drives to be removable, particularly for classified processing. The policy should require all new procurements to specify removable hard disk drives, and all existing systems to be retrofitted with removable hard disk drives. The migration to removable hard disk drives is encouraged because they:

a. Reduce the need for open storage and continuous personal supervision of computers that process classified information;

b. Simplify system declassification for maintenance, field and travel use, emergency destruction, and end-of-life-cycle disposal;

c. Facilitate periods processing;

d. Facilitate multi-purpose use in changing environments;

e. May simplify requirements for relocating desktop systems during office reorganizations

2. *Periods Processing* is a manner of operating an Automated Information System (AIS) in which the security mode of operation and/or maximum classification of data handled by the AIS is established for an interval of time (or period) and then changed for the following interval of time. A period extends from any secure initialization of the AIS to the completion of any purging of sensitive data handled by the AIS during that period. Each command must have a procedure for periods processing (dual use) computers. The use of a notebook computer in a classified environment and then in an unclassified environment (or vice versa) requires the implementation of the following steps, to include sanitation/purging/clearing:

a. The computer must be turned off (i.e., powered off). This step is required to ensure that temporary storage (e.g. RAM) is cleared. If the notebook has the ability to maintain RAM (e.g., flash RAM), that process must be disabled or you can not do periods processing.

b. The system must be put in a stand alone posture. All external peripherals must be disconnected. (e.g. network, printer, modem, scanner). The storage media (e.g. hard disk) then can be swapped with the appropriate media (changing a hard drive on some notebook computers is not a trivial task). The media must be marked with the proper classification label and be appropriate for the system's intended environment.

c. The suitable peripherals (they may also require clearing) may then be connected to the system and the system can now be used in the new environment.

d. The mode of operations MUST BE READILY APPARENT TO THE USER (I.E., THE USER MUST EASILY RECOGNIZE THE ENVIRONMENT). This can be done electronically (e.g. different operating systems, different screen backgrounds and different colors, labels on the screen) or by physical markings (e.g. computer labels).

e. The System Security Plan (SSP) addressing the system must cover all modes of operation. The user must be aware of the procedures for changing into the different environments.

APPENDIX C – ADDITIONAL SECURITY OPTIONS

Annex D – Privately Owned Computer Systems

1. Use of privately owned computer systems for official government business is discouraged. Commands that decide to allow the use of privately owned computer systems must have a policy governing the use of such systems. All use of privately owned computer systems shall be approved by the cognizant DAA. At a minimum a policy for the use on privately owned computer systems must address the following:

a. The risk to government information.

b. The possible loss of use of system resources or productivity if the system should become contaminated with Government Interest information, classified or unclassified.

c. The procedures to be followed by the appropriate security official in the case of system contamination include:

(1) How to report such a contamination

(2) Rules to be followed to preserve chain of evidence

(3) The recovery procedures to be followed

(4) How non-government files or media shall be protected and how access to these files, if not contaminated with Government Interest information, shall be provided to the owner in an expeditious manner.

2. In no case shall a privately owned computer system be used to process, transmit, or store classified or sensitive unclassified information.

3. Direct connection of privately owned laptops, personal (pocket) organizers, data link watches and other similar devices to government computer systems is discouraged. The determination to allow connections shall be made on a case by case basis by the cognizant system DAA. There should be a standard agreement signed by anyone using a privately owned system for work-related purposes. It should state that signing the agreement constitutes consent to sysadmin inspection, temporary possession and the personal assumption of risk for any damages that may result from attempts to clear government-owned information from the personal property.

4. Copying software. Public Law 94-553, Copyright Act of 1976, codified as amended at Title 17 United States Code provides the basis for the following requirements:

a. It is forbidden to make unauthorized copies of commercially acquired and/ or proprietary software in which the U.S. government has restricted and unrestricted rights of use of duplication.

b. It is forbidden to use a government computer system to make unauthorized copies of any commercially acquired and/or proprietary software.

c. Use of privately owned or privately licensed software on government systems is forbidden, with exceptions to be permitted only in accordance with the software license and with the prior approval of the cognizant system DAA.

d. Questions on the authorized use and copying of software should be directed to the cognizant system security officer.

e. All computer users and system administrators, as appropriate, have an ethical and legal responsibility to ensure that commercial computer software is used for its intended purposes.

APPENDIX D – DEFENSIVE INFORMATION OPERATIONS

1. Role of Defensive Information Operations. Commands shall have flexible, realistic deployment plans which ensure that Information Assurance and Defensive Information Operations are factored into all peacetime, contingency, combat, or coalition planning and operations for every system subject to deployment or connectivity to a deployed location. Command DAAs should specify in the system security accreditation letter that a system can be deployed and operated in accordance with the deployment plans. Deployment plans should address the following security points:

a. The person or offices authorized to order deployment of the system.

b. Additional security approvals required for deployment and the office responsible for getting them.

c. Requirements for deployed ISSOs. All deployment plans with requirements for deployed ISSOs shall ensure that ISSOs have received proper training, prior to deployment, in related disciplines. This training should include, but is not limited to: Network Security Officer, Security Life Cycle Manager, System Administrator, and Configuration Manager. The need for such training is to ensure that deployed ISSOs are prepared to handle any situation they may encounter.

d. Secure transport of the system to the deployment site, and secure return transport to garrison.

e. Physical security of the system at the deployment site.

f. System configuration changes required for deployment.

g. COMSEC and Protected Wireline Distribution System (PDS) requirements at the deployment site.

h. Secure installation and maintenance at the deployment site.

i. Verification of the security clearances of new users at the deployment site, and essential user security training.

j. Emergency destruction plans for the deployment site.

k. Plans for restoration / reconstitution of the system and infrastructure.

l. Multinational / coalition networking considerations.

2. COMSEC. Commanders are responsible for ensuring the security of information transmitted over their communications systems and media. At a minimum, commanders must consider:

a. Availability of appropriate COMSEC equipment and keying material

b. Personnel training in use of COMSEC equipment and in the requirements for when to use COMSEC devices or systems

c. Cryptonetting requirements

d. Requirements for release of COMSEC devices to foreign nationals for interoperability, as stated in CJCSI 6510.01B

2. Travel. Commands shall ensure that all persons are aware of and have had training in proper information system security procedures and their information assurance responsibilities to ensure proper protection of information and information systems while traveling. This training should also include procedures for reporting possible security incidents, required use of encryption systems, and other IA measures. Special consideration should be given to travel in high risk areas; consult your local force protection office.

APPENDIX D – DEFENSIVE INFORMATION OPERATIONS

Annex A – Information Conditions (INFOCONS)

1. (U) This Annex establishes the minimum requirements for the USEUCOM Information Operations Condition (INFOCON) levels. These INFOCON typify threat Information Operations (IO) activity at each INFOCON level, and corresponding response measures to increase the defensive IO readiness of the entire theater or a specific sub-region, depending on the IO threat. INFOCONS are based on a combination of threat, vulnerabilities, incidents, and real-world conditions. The USEUCOM INFOCONS are applicable to all USEUCOM forces, including Component Commands, Subordinate Unified Commands, and Joint Task Forces (JTF).

2. (U) Commands in USEUCOM present an opportune target for an attack on our information infrastructure. Our information vulnerabilities can be exploited by a host of potential "adversaries", including: novice computer hackers, disgruntled employees, non-state actors, and nation-state sponsored organizations. Our information infrastructure includes traditional communications systems (telephones, SATCOM, INMARSAT, etc.), many of which are carried over the public switched network, computer networks, and other automated or electronic systems used to process our communications and information flow. It can also include things such as power generation, transportation, water supply, or other non-DoD infrastructure that can affect USEUCOM's ability to perform its mission. These information system vulnerabilities demand an aggressive Defensive IO and Information Security (INFOSEC) strategy to ensure our combat readiness.

3. (U) The decision to increase the defensive IO posture for the theater, or to increase the INFOCON level, is not a stand-alone process. In fact, the process is very much integrated with established procedures and organizations. USEUCOM establishes the theater INFOCON based on important assessments provided by the Operations, Intelligence, and Command, Control, Communications, and Computer (C4) Communities. The C4 community provides both global and theater assessments of computer network intrusion incidents. The Defense Information Systems Agency - Europe (DISA-EUR), through its Regional Operations and Security Cell (ROSC), consolidates theater computer intrusion incidents and provides assessments to both HQ USEUCOM and HQ DISA. Additionally, DISA's Global Operations Support Center (GOSC) provides worldwide assessments to HQ USEUCOM, through DISA-EUR. The National Security Agency (NSA) provides SIGINT threat information and reports that correlate global DoD intrusions and intelligence information to HQ USEUCOM. Various Service intelligence and Computer Emergency/Incident Response Teams, DIA, JAC Molesworth, the Joint COMSEC Monitoring Activity (JCMA), and others also provide information important to evaluating vulnerabilities and threats to our information systems. In addition to these inputs HQ USEUCOM receives PSYOP and foreign media/information assessments, when appropriate. INFOCON levels may also change as an anticipated response to current or planned friendly operations or activities. All of these assessments (threat, vulnerability, intelligence, C4, PSYOP,

foreign media/information, friendly operations, etc.) are ultimately forwarded to HQ USEUCOM Information Operations Cell (IOC) (as described in ED 100-1. Once a change in INFOCON level is declared the new INFOCON will be transmitted to the Components, Subordinate Unified, and JTF Command Elements for implementation. HQ USEUCOM will also inform the Joint Staff of the change in USEUCOM's INFOCON level.

4. (U) INFOCONs: INFOCON levels are NORMAL, ALPHA (Low Activity), BRAVO (Significant Activity), CHARLIE (Serious Activity), and DELTA (Critical Activity). INFOCON levels are analogous to DEFCON, WATCHCON, and THREATCON levels but can vary in their application. Although events that would raise or lower those levels may directly affect the existing INFOCON level, USEUCOM could declare a higher or lower INFOCON level without the declaration of a similar DEFCON, WATCHCON, or THREATCON level change.

a. (U) USEUCOM ECJ3 is the INFOCON declaration authority within USEUCOM. Establishing an INFOCON does NOT presuppose all response measures within the declared INFOCON will be activated. Upon declaration of INFOCON ALPHA or higher, HQ USEUCOM will direct specific defensive measures for implementation within the theater (e.g. response measures A-2, A-5, A-14, etc). Directed action may include measures from a higher INFOCON. For example, while in INFOCON ALPHA, HQ USEUCOM may direct measures listed in INFOCON BRAVO. HQ USEUCOM directed measures do not preclude Component, Subordinate Unified, JTF, or local Commanders from initiating more restrictive action, if desired. However, commands must remain at least as high as the current INFOCON directed by USEUCOM.

b. (U) Component, Subordinate Unified, and JTF Commanders who receive conflicting INFOCON guidance from another Unified Command or Service will inform HQ USEUCOM IOC. Within the USEUCOM AOR, USEUCOM INFOCONSs take precedence.

c. (U) The decision to change INFOCON levels will be based on assessed threat, vulnerabilities, extant situation, and the effect the action would have on all operations within the USEUCOM AOR. ECJ2 will advise HQ USEUCOM of the assessed threat, and ECJ6 will advise on vulnerabilities. IOC, in coordination with the IO Cell Working Group, will recommend changes in INFOCON level to the USEUCOM ECJ3.

d. (U) If appropriate, INFOCON response measures may be directed for implementation within a specific sub region within the USEUCOM AOR, or theater-wide. They may also be directed based upon the situation in other CINC AORs, since threat activities in other regions could have an impact on USEUCOM AOR operations.

e. (U) Response measures are directive and do not simply provide information security advisories. As discussed in paragraph 4(a) above, response measures may be directed for implementation individually (e.g., implement response measures A-2, A-3, and B2), or response measures may be grouped together (e.g., implement all INFOCON BRAVO response measures).

f. (U) INFOCONS and response measures apply to all official USEUCOM networks, to include Secure Internet Protocol Routing Network (SIPRNET), and NIPRNET networks. SCI networks will also comply with USEUCOM INFOCONS to the maximum extent possible, with notification and concurrence by the cognizant authority for each SCI network.

g. (U) The threat IO activity described in each INFOCON, and the corresponding responses are not all inclusive. Each Component, Subordinate Unified, and JTF Command should review these measures for applicability and determine if additional response measures are required. Additionally, as technology changes, these measures should be reviewed periodically to account for vulnerability changes.

h. (U) Each Component, Subordinate Unified, and JTF Command should promulgate amplifying instructions for all response measures, if required. The IO Cell will provide any amplifying instructions for use within HQ USEUCOM. Any exceptions to INFOCON Measures will be coordinated through the IOC.

i. (U) Paragraph 5 below describes typical threat activity for each INFOCON. These are used only as guidelines in declaring a particular INFOCON. For example, while insertion of malicious code and viruses are typical threat activity listed under INFOCON CHARLIE, USEUCOM may elect to remain in INFOCON BRAVO due to the specific situation.

5. (U) INFOCON LEVELS

a. (U) INFOCON NORMAL. This day-to-day condition warrants established routine security procedures. Typical threat IO activity at this level includes random surveillance or reconnaissance probes on USEUCOM's information infrastructure as detected by network automated intrusion detection systems (IDS). Vulnerabilities are assumed to be consistent with those documented in the system security documentation for each computer network, or in previous assessments of other communications systems. No special alerts or advisories have been received from any DoD Agencies indicating a specific threat or new vulnerabilities. Foreign press and public diplomacy activities are routine. At this level, daily information system security measures apply including automated 24 hour/day monitoring of critical command, control, and communication systems. DISA-EUR's ROSC provides 24 hour/day monitoring of non-SCI systems. Cognizant authorities for SCI or other systems conduct system intrusion monitoring per their own procedures.

b. (U) INFOCON ALPHA (Low Activity). This condition is declared when a general threat of information attack against USEUCOM exists. Typical threat IO activity at this level includes computer network scans, probes, or mapping, increased foreign SIGINT targeting of our communications systems, any I&W or intelligence indicators of planned or increased threat activities which might indicate an increased surveillance or reconnaissance against USEUCOM's information infrastructure, planned operations, contingency or exercises ongoing, or major regional events that affect U.S. interests. Limited computer network attacks, with no operational impact, could also be expected at this INFOCON level. Other forms of threat IO activity could include public diplomacy efforts by an adversary to undermine U.S. regional interests and policy.

Vulnerabilities are assumed to be consistent with those documented in the SSAA for each computer network, or in previous assessments of other communications systems. Special alerts or advisories have been received from DoD Agencies indicating a general threat or new vulnerabilities may be existent. The measures for this INFOCON must be capable of being maintained indefinitely.

c. (U) INFOCON BRAVO (Significant Activity). This condition is declared when a specific threat of an information attack against USEUCOM exists. This condition may be prompted by an information warfare (IW) threat warning assessment indicating specific adversary capabilities with evidence of intent. Typical threat IO activity at this level includes limited computer network attacks with minor operational impact, increased foreign SIGINT targeting of USEUCOM communications systems, limited electronic warfare harassment or attacks with minor operational impact. Additional indicators include: increased anti-U.S./western rhetoric, leaflet campaigns, public demonstrations, public speakers, "Internet rumors," or media reports counter to U.S., U.S. allies, or U.S. coalition partners. Other indicators may include a significant increase in detected viruses, or limited denial of service attacks. Not all of the above activities need occur for declaration of INFOCON BRAVO, and some of the activities may be occurring in other Theaters, but have the potential for impact on USEUCOM operations. At this level, new or existing vulnerabilities must be identified and actions taken to mitigate them. These measures should be able to be maintained for several weeks without undue personnel hardships or degrading USEUCOM's ability to operate.

d. (U) INFOCON CHARLIE (Serious Activity). This condition applies when an actual information attack occurs or when intelligence indicates the possibility of an imminent information attack that could result in a significant operational impact. Typical threat IO activity at this level includes actual or threatened attempts to gain access to USEUCOM computer network systems for the purpose of massive data destruction, false data creation, wide denial of service, or gaining control of critical systems. The injection across several networks of malicious code, viruses, Trojan horses, and e-mail bombs all fall into this INFOCON. It further includes known SIGINT targeting and/or electronic warfare (EW) attacks against USEUCOM communications systems, or specific threats to and vulnerabilities of those communications systems. At this INFOCON level, entities acting either singularly, aligned, or in unprecedented coalitions, can be expected to counter U.S. policy through intense and broad regional press and public diplomacy. Limited hostile military force relocation or realignment, hostile economic activities or actions, or other social, political, or military actions could be involved. This INFOCON could also be declared when U.S. information systems are under attack from non-state groups or organizations. Response measures at this INFOCON are focused at protecting USEUCOM forces' ability to operate as needed on critical systems. When implemented for even short periods of time, response measures at this INFOCON could create personal hardship, affect peacetime capabilities, and have the potential for increased operational costs.

e. (U) INFOCON DELTA (Critical Activity). This condition applies when the global situation has led to increases in DEFCON, WATCHCON, or THREATCON levels which warrant extreme measures, or when the severity of an information attack against USEUCOM significantly degrades readiness and operations. Extensive coordinated regional and global

information attacks by entities with hostile intent toward/against the U.S. and its allies are expected, and could include computer system attacks, hostile SIGINT or EW activity , and utilization of known vulnerabilities for coordinated attacks on U.S. information systems, including hostile media attacks which are counter to U.S. policy and interests. Response measures at this INFOCON are focused on maintaining or restoring USEUCOM's ability to operate its minimum critical systems. As with INFOCON CHARLIE, the response measures will likely result in personal hardships, increased operational costs (both time and dollars) and a degradation in peacetime capabilities.

6. (U) INFOCON RESPONSE MEASURES

a. (U) INFOCON ALPHA (Low Activity)

(1) (FOUO) Measure A-1: Notify all members of the USEUCOM IO Working Group via telephone and/or e-mail to inform them of the IO activity, and immediate actions being taken. (IOC)

(2) (FOUO) Measure A-2: Verify USEUCOM IO point of contact list of phone numbers, e-mail addresses, and official message traffic address list. (IOC)

(3) (FOUO) Measure A-3: Alert ECJ2 to monitor threat for additional DIO indications and warnings (I&W), and increased foreign intelligence and information activity. ECJ2 to notify national intelligence agencies of same, and request increased vigilance and reporting from them. (IOC/ECJ2)

(4) (FOUO) Measure A-4: Issue threat assessments of suspected IO activities and organizations and identify suspected friendly targets of any IO attacks (ECJ2)

(5) (FOUO) Measure A-5: Issue daily status report of DIO activities to the Joint Staff with information copies to the Components, Subordinate Unified, and JTF Commands. (IOC)

(6) (FOUO) Measure A-6: Issue daily status report of DIO activities to the USEUCOM IOC in accordance with report format in Para 7. (Component, Subordinate Unified, and JTF Commands)

(7) (FOUO) Measure A-7: Ensure all Security Managers, Information System Security Managers (ISSM), Information System Security Officers (ISSO), System Administrators (SA), COMSEC Custodians, and other communications or information systems organizations or personnel (e.g. 52nd Signal Brigade) are briefed on the threat IO activity, INFOCONS changes, and response measures. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands.)

(8) (FOUO) Measure A-8: Issue an e-mail to remind all personnel to increase OPSEC awareness. Include things such as reminding all users of the risks of being monitored by

adversaries during e-mail and phone use (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(9) (FOUO) Measure A-9: Remind all users to immediately report anyone requesting direct access or computer passwords to access C4I networks and workstations. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(10) (FOUO) Measure A-10: Remind all users that scanning computer floppy disks for viruses is mandatory prior to use in USEUCOM computers. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(11) (FOUO) Measure A-11: Remind all users to report unusual activity, viruses, and potential denials of service of computer, radiotelephone, satellite, or telephone systems (including FAX machines). Report unusual activity in accordance with established USEUCOM and local incident reporting procedures. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(12) (FOUO) Measure A-12: ISSM, ISSO, and SA will remind users of the need for passwords with a minimum of 8 random alphanumeric characters. This is to counter attempts to crack passwords with very large dictionary word files. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(13) (FOUO) Measure A-13: Ensure all dial-in/dial-out capabilities are removed from LAN workstations. Only stand-alone workstations will be used for Fax and answering machine capabilities. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(14) (FOUO) Measure A-14: Update and distribute list of intruder Internet Protocol (IP) addresses for local IP hotlists. (ECJ2 CSG from NSA SIPO)

(15) (FOUO) Measure A-15: Update IW attack signatures, profiles, and methods of recent attack for use by intrusion detection systems, and for use by SA to manually detect intrusions. (DISA-EUR/NCEUR)

(16) (FOUO) Measure A-16: SA will update all virus software and DAT files. All workstations will be scanned for viruses. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(17) (FOUO) Measure A-17: SA will validate the operation of server system log files, and in addition to daily reviews, review firewall and intrusion detection logs for evidence of specified unusual or malicious activity. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(18) (FOUO) Measure A-18: If threat source is known, SA will ensure routers and/or firewalls block appropriate Internet Protocol (IP) hotlist address listings. Monitor and log activity as appropriate. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(19) (FOUO) Measure A-19: SA will ensure routers and firewalls protecting all segmented critical C4I networks have proper configuration settings to guard against known vulnerabilities and methods of recent attacks. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(20) (FOUO) Measure A-20: Assess composition of interagency, Directorate, and Component or JTF participation in HQ's USEUCOM IO Working Group. (IOC)

(21) (FOUO) Measure A-21: Ensure all telephone instruments are at least 3 feet from computers handling classified material. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(22) (FOUO) Measure A-22: Monitor media for indicators of coordinated campaign to manipulate coverage against the U.S. and its allies. (ECPA)

(23) (FOUO) Measure A-23: Direct all users to conduct a STU-III key update with the Key Distribution Center (DSN 550-7883) to obtain the latest Compromised Key List (CKL). (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(24) (FOUO) Measure A-24: SA require all computer systems users to change passwords within 48 hours. Passwords will be changed every 90 days while in INFOCON Alpha. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(25) (FOUO) Measure A-25: All USEUCOM elements will ensure that USCINCEUR//ECJ6-I// is an info addressee on all COMSEC incident reports. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(26) (FOUO) Measure A-26: ISSO/ISSM locate and verify current status of all accreditation packages. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(27) (FOUO) Measure A-27: MLS/SABI Action Officers verify current list of all MLS or SABI interconnections, and status of accreditation packages for same to HQ USEUCOM MLS/SABI Action Officer. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(28) (FOUO) Measure A-28: After Measure A-24 is implemented, SA will run password cracking tools against system password databases to ensure compliance with Measures A-12 and A-24. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(29) (FOUO) Measure A-29: Verify and report application of all known and approved operating system patches, fixes, and new releases to the USEUCOM ISSO/ISSM. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

b. (U) INFOCON BRAVO (Significant Activity)

(1) (FOUO) Measure B-1: Ensure all Alpha measures are implemented as directed. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(2) (FOUO) Measure B-2: Develop/update IO target folders (e.g., command and control and news media networks). (ECJ2)

(3) (FOUO) Measure B-3: Direct all ISSM, ISSO, and SA to increase their security awareness, particularly for critical C4I systems, and place them on alert for possible recall after normal duty hours. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(4) (FOUO) Measure B-4: DISA-EUR, NCEUR, ECJ6-I and ECJ2 will coordinate to establish a consolidated system security analysis effort for continuous (24 x 7) operations. This effort will update current adversaries IO attack signatures, and compare those signatures to known friendly vulnerabilities of computer- and communications-based information systems. (DISA-EUR, NCEUR, ECJ6-I and ECJ2)

(5) (FOUO) Measure B-5: All COMSEC Incident reports will be evaluated by the EUCOM ECJ6-I for potential DIO implications. Those incidents that may have potential DIO implications will be referred to the IO Cell. (ECJ6)

(6) (FOUO) Measure B-6: SA will force all users to enter new passwords. ISSMs, ISSOs, and SAs will remind users of the need of passwords with a minimum of 8 random alphanumeric characters. Passwords will be changed at least every 30 days as appropriate. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands.)

(7) (FOUO) Measure B-7: Monitor incoming, outgoing, and switch-to-switch telephone trunks for call completion rate, and grade of service. (ECJ6)

(8) (FOUO) Measure B-8: Close all remote maintenance ports on vulnerable or affected routers, firewalls, servers, computer-based telephone switches, and any other accessible information systems. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(9) (FOUO) Measure B-9: Verify real-time audit analysis capabilities, if available, are turned on and monitored. Alarm levels of Automated Intrusion Detection Systems should be adjusted to provide appropriate alert thresholds. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(10)(FOUO) Measure B-10: Task the Joint COMSEC Monitoring Activity to begin monitoring and reporting of all USEUCOM INMARSAT Terminals, line-of-sight (VHF and HF) communications from JCMA garrison sites. (ECJ6)

(11)(FOUO) Measure B-11: Develop a plan for JCMA COMSEC monitoring support for HQ USEUCOM and components telephones, cell phones, and e-mail networks. (ECJ6)

(12) (FOUO) Measure B-12: Review options, and operational impacts of, disconnecting all MLS or SABI bridges between classified and unclassified networks and/or between classified and allied networks, such as the Secure Mail Guards (SMG). (HQ USEUCOM IOC & ECJ6; Components, Subordinate Unified and JTF Commands)

(13) (FOUO) Measure B-13: SA's will reduce dial-in access on both the U-LAN and S-LAN to minimum essential personnel as directed by ECJ3. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(14) (FOUO) Measure B-14: SA will reduce user access to U-LAN via the Webpage to minimum essential personnel as directed by ECJ3. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands).

(15) (FOUO) Measure B-15: Conduct computer network vulnerability assessments to re-verify levels of information security. For example, request that DISA-EUR run the STIG (Secure Technical Implementation Guideline) software on the HQ USEUCOM U-LAN. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands with support from DISA-EUR and NCEUR)

(16) (FOUO) Measure B-16: For the conduct of official business, use only approved secure modes of information exchange, such as secure telephones (STU-III), secure FAX, and SIPRNET-based systems such as Global Command and Control System (GCCS). (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(17) (FOUO) Measure B-17: Notify post/base/camp law enforcement and emergency personnel of INFOCONS status. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(18) (FOUO) Measure B-18: Respond to false or distorted reports regarding the U.S. or its allies or coalition forces from foreign media or information sources. (ECPA)

(19) (FOUO) Measure B-19: Direct discontinuance of 'sneaker net' transfers of information between computer workstations via floppy disk unless disk has been virus scanned. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(20) (FOUO) Measure B-20: Remove all hard drives from workstations not in use. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(21) (FOUO) Measure B-21: SA will review network monitoring logs, system audit logs, and server system log files for evidence of specified unusual or malicious activity. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(22) (FOUO) Measure B-22: SA to begin keeping detailed activity logs for all actions taken and information received. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(23) (FOUO) Measure B-23: If available, implement alternate FAX numbers in response to denial of service attacks on FAX. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(24) (FOUO) Measure B-24: HQ USEUCOM IOC goes to continuous (24 x 7) manning. (IOC)

(25) (FOUO) Measure B-25: Activate the HQ USEUCOM Crisis Action Team (CAT). (ECJ3)

(26) (FOUO) Measure B-26: Post guards on secondary power generation equipment for critical command and control centers within USEUCOM. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(27) (FOUO) Measure B-27: Develop final plan for configuration settings for all firewalls, routers, filters, and guards for INFOCON CHARLIE implementation. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

c. (U) INFOCON CHARLIE (Serious Activity)

(1) (FOUO) Measure C-1: Ensure Alpha and Bravo measures are implemented as directed. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(2) (FOUO) Measure C-2: In the case of an actual computer network attack, users of the affected workstations, and the respective ISSM and ISSO, will isolate the affected workstation or network, ensure evidence is maintained to pass to law enforcement agencies, and then attempt to clean and recover the workstation/network. This measure will only be accomplished following a decision by the ECJ3 as to what response or other active measures may be implemented, unless a minimum critical system is at immediate risk. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(3) (FOUO) Measure C-3: Disconnect Secure Mail Guards (SMG) or any other SABI or MLS device between unclassified and classified LANs. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(4) (FOUO) Measure C-4: Review current IDS coverage and expand to additional computer networks, if operationally feasible. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(5) (FOUO) Measure C-5: Initiate plan from B-11 for JCMA COMSEC monitoring support of HQ USEUCOM telephones, cell phones, and computer networks. (ECJ6)

(6) (FOUO) Measure C-6: Disconnect all terminals and workstations not in use. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(7) (FOUO) Measure C-7: Disconnect any non-mission essential MLS or SABI connections between classified and allied networks. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(8) (FOUO) Measure C-8: Review options, and impacts of, disconnecting all critical C4I systems, networks and workstations capable of operating in a stand-alone mode. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(9) (FOUO) Measure C-9: Form a combined (Component, Service law enforcement offices, FBI) interagency "IO Response Board". (IOC)

(10) (FOUO) Measure C-10: Develop or update adversary IO targets for potential courses of active response action and objectives, and determine availability and feasibility for preemptive IO attacks through various means (e.g., PA, military deception, OPSEC, PSYOP, EW, and physical destruction). (IOC)

(11) (FOUO) Measure C-11: Disconnect all subnetworks from the HQ USEUCOM classified LANs. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(12) (FOUO) Measure C-12: Request immediate vulnerability assessment of any remaining operational interconnections. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(13) (FOUO) Measure C-13: Request immediate TSCM/TEMPEST site evaluation for potential vulnerabilities. (ECJ6)

(14) (FOUO) Measure C-14: Conduct review of all COMSEC key management plans, and prepare implementation of full rekey of minimum critical networks and systems. (ECJ6)

(15) (FOUO) Measure C-15: Implement manned 24x7 monitoring of all network servers, guards, filters, firewalls and other activity logs for suspicious or unusual activity. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(16) (FOUO) Measure C-16: Implement plan from Measure B-27 for configuration settings for all firewalls, routers, filters, and guards. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(17) (FOUO) Measure C-17: As appropriate, re-adjust alarm levels of Automated Intrusion Detection Systems to provide appropriate alert thresholds. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(18) (FOUO) Measure C-18: SA will deny ALL access to the U-LAN Web servers. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(19) (FOUO) Measure C-19: SA will configure firewalls to allow access to only approved, official addressees (i.e. gov, mil, etc) as directed by J-3. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(20) (FOUO) Measure C-20: SA will remove ALL dial-in access to U-LAN. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

(21) (FOUO) Measure C-21: SA will remove ALL dial-in access to S-LAN. (HQ USEUCOM, Component, Subordinate Unified and JTF Commands)

d. (U) INFOCON DELTA (Critical Activity)

(1) (FOUO) Measure D-1: Ensure Alpha, Bravo, and Charlie measures are implemented as directed. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(2) (FOUO) Measure D-2: Provide input to plans to destroy adversaries IO capabilities for protection purposes, to include: physical attack, PSYOP, EW, and CNA. (IOC)

(3) (FOUO) Measure D-3: Develop or update plans to counter adversary's strategic propaganda and deception campaign. (IOC)

(4) (FOUO) Measure D-4: SA will disconnect ALL NIPRNET access on U-LANs. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(5) (FOUO) Measure D-5: SA will disconnect ALL SIPRNET access on S-LANs. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

(6) (FOUO) Measure D-6: Disconnect all critical C4I systems, networks and workstations capable of operating in a stand-alone mode. (HQ USEUCOM, Component, Subordinate Unified, and JTF Commands)

7. (U) REPORTING

a. (U) HQ USEUCOM IOC will inform Component, Subordinate Unified, and JTF Commands upon USEUCOM declaration of a change in INFOCONS level, or when Component, Subordinate Unified, and JTF Commands initiate more restrictive response measures. HQ USEUCOM IOC will also inform Component, Subordinate Unified, and JTF Commands of specific response measures taken within theater, and of the activity that warranted implementation of those response measures. Primary reporting means will be via official message traffic.

b. (U) Component, Subordinate Unified, and JTF Commands will notify HQ USEUCOM IO Cell (IOC) when response measures are implemented, to include measures taken but not directed by USEUCOM.

c. (U) HQ USEUCOM IOC will notify the ECJ3 whenever any INFOCONS response measures are implemented within USEUCOM.

d. (U) HQ USEUCOM IOC will inform the Joint Staff ECJ39 of USEUCOM INFOCONS status, and response measures taken.

e. (U) Reporting Frequency: Status report will be sent within two hours of direction to change INFOCONS. During duty hours notification will be made to IOC at DSN 430-4233/ 5638/5163. During non-duty hours, notification will be made to IOC through the USEUCOM Theater Command Center (ETCC) at DSN 430-5067.

f. (U) Report Formats: Reports of changes in INFOCONS should be accompanied by an operational assessment of the situation when appropriate. Annex D, ED 25-5 outlines a process for assessing the operational impact of a computer network attack. Reports will include, as a minimum:

(1) (U) For all INFOCONS: Unit/organization and location, date/time of report, current INFOCON, reason for declaration of this INFOCON, current status of each INFOCON measure taken, POC (name, rank, duty title, contact information)

(2) (U) INFOCON CHARLIE and higher: All of the above, including: system(s) affected (network, classification, application, database/data file), degree to which operational functions are affected (C2, ISR, movement/maneuver, sustainment, fires, protection), impact (actual and/or potential) on current/planned missions and/or general capabilities, restoration priorities, workarounds.

8. (U) Classification Guidance. Definitions of INFOCONS levels are unclassified. The listing of response measures linked to a specific INFOCONS level or specific IO threat, are classified FOUO. Implementation of any INFOCON measures when directed by a competent authority will be classified Confidential or higher depending on the content or mission.

9. (U) Comments and Recommendations. Direct all comments and recommendations concerning these INFOCONS to HQ USEUCOM IOC.

(This page intentionally left blank)

APPENDIX D – DEFENSIVE INFORMATION OPERATIONS

Annex B – Incident Reporting Process

1. Incident reports allow local, regional and global authorities to detect and respond to coordinated attacks, therefore timely and accurate incident reporting is critical. Commanders at all levels are responsible for establishing incident reporting procedures within their AOR, and are further responsible for establishing procedures to notify supporting intelligence and law enforcement organizations. Information Assets include data, information-based processes, information systems, and information transfer links and mechanisms. An Information Event is any pre-assessed suspicious or anomalous activity affecting an information asset. An Information Incident is an assessed information event indicating an adversarial attack on an asset. As a minimum, all information events and incidents affecting USEUCOM information assets shall be reported using the procedures described below.

a. Any user noticing anomalous or suspicious activity shall report the situation to his Local Control Center (LCC). Users shall report events as they occur, or as they are recognized.

b. LCCs noting an information event or incident shall issue a report to DISA's Regional Operations and Security Center – Europe (ROSC-EUR), the appropriate service CERT or CIRT, and supporting law enforcement and intelligence organizations in accordance with local procedures. Information events and incidents should be reported as they occur, with the exception of isolated and controllable computer viruses, which can be reported weekly. Reports should be distributed in as timely a manner as is possible, even if the initial reports are brief.

c. Service CERTs and CIRTs detecting information events or incidents affecting USEUCOM assets shall report them to the affected LCC and ROSC-EUR.

2. ROSC-EUR is responsible for gathering all event and incident reports for the USEUCOM AOR and performing analysis to generate and assess the status and welfare of the region's information environment. ROSC-EUR shall report information events and incidents in the CINC AOR to the CINC staff and local intelligence and law enforcement agencies in accordance with locally developed procedures. ROSC-EUR shall also, in coordination with the USEUCOM ECJ3, provide situational awareness information concerning incidents occurring in the USEUCOM AOR to elements within the AOR and lateral ROSCs.

3. Information event or incident reports shall contain applicable classification markings and caveats (as determined by the applicable Security Classification Guidance), basic contact information, Minimum Essential Elements of Information (who, what, when, where, why and how), and the action taken. Security Classification Guidance shall be developed and disseminated through the DISA GOSC, and in the absence of specific guidance all reports shall be treated as For Official Use Only as a minimum.

(This page intentionally left blank)

APPENDIX E – ALLIED SECURE INTEROPERABILITY RELEASE REQUESTS

1. Whenever any entity determines that a non-NATO country in the USEUCOM AOR shall require the provision of COMSEC equipment and/or keying material in order to securely interoperate with USEUCOM or other U.S. forces, they shall provide, by electrical message, a statement of the need for such release to USEUCOM ECJ5 with info copy to ECJ6-I. (Internal USEUCOM staff directorates may use an SSRS for stating the requirement).

2. The appropriate ECJ5 Country Team shall evaluate the requirement and determine if there is a supporting Operations Plan or Concept of Operation Plan that applies to secure interoperability requirements with the country in question.

3. If there is documentation that supports a secure interoperability requirement, ECJ5 shall draft and staff a message to the Joint Staff ECJ6I with info copy to DIRNSA I11 requesting a release-in-principle of the required COMSEC equipment and keying material for the country in question.

4. Once the release-in-principle is approved by the NSTISSIC and message approval is received from the Joint Staff, the entity that originally determined the requirement is responsible for gathering the following information from the country in question. This information shall help ECJ6-I determine if the requirements in Appendix D, Annex D of CJCSI 6510.01 for safeguarding the COMSEC equipment and keying material can be met by the country in question.

a. Copies of any relevant COMSEC storage, handling or use policy and execution documents from the country.

b. Description of specifically who in the country shall receive, store and use the COMSEC equipment and material.

c. Drawings or descriptions of the areas where COMSEC equipment and keying material shall be stored.

d. Plans on how the equipment shall be installed and maintained.

e. Details of who in the country would be responsible for negotiating a Memorandum of Agreement and any other required agreements in order to implement a COMSEC release to them.

5. Upon receipt of the information in para 4, above, ECJ6-I shall evaluate the capability of the country to properly receive, store and use U.S. COMSEC equipment and material. If the country can meet the necessary requirements, ECJ6-I shall release an electronic message to the Joint Staff ECJ6I formally requesting release of the specific equipment and material to the country, and requesting authority for the originating entity to negotiate and conclude a formal Memorandum of Agreement and other necessary documents with the country.

6. Upon receipt of DIRNSA and Joint Staff approval to negotiate and conclude an agreement with the country, ECJ6-I shall provide the originating entity a copy of a draft MOA and other necessary documents that has been approved by DIRNSA for release of COMSEC material and equipment.

7. The originating entity shall then negotiate the MOA and other necessary agreements with the country. As long as no substantive changes are made to the approved MOA or documents, the originating entity shall provide the final versions of the documents to ECJ6-I.

8. ECJ6-I shall review and provide the documents to ECJ5 for staffing and signature by the appropriate USEUCOM signature authority.

9. Once signed, ECJ5 shall provide copies of the signed agreements to ECJ6-I for provision to DIRNSA and the Joint Staff and for record purposes.

10. The originating entity shall then work with DIRNSA I11 to effect the provision, installation, training, and operation of the equipment and material to the country, keeping USEUCOM ECJ5 and ECJ6-I informed as to all activities to effect the release.

APPENDIX F – BULK ENCRYPTION POLICY

1. Purpose. This enclosure prescribes policy and procedures for the planning and implementation of bulk encryption within the European theater. Bulk encryption shall ensure sensitive unclassified information is protected during transmission to prevent its disclosure, misuse, alteration, destruction or non-availability ensuring to the user the information has maintained its integrity.

2. Definitions

a. Bulk encryption is defined as the simultaneous encryption of two or more telecommunications channels that have been electronically multiplexed together. In practice, bulk encryption involves the encryption of any composite data stream between DCS end stations.

b. Link encryption is defined as the encryption of a single telecommunications link at the highest composite rate by on-line, encryption devices at the injection point into a DCS multichannel transmission system. In practice, link encryption involves the encryption of all data between two sites/stations.

c. Source encryption is defined as the encryption of a single telecommunications circuit by on-line encryption devices at the source of the data stream generation. In practice, source encryption involves the encryption of any data stream between generating source and the receiving end.

d. Guided media is defined as a transmission path, fully contained by a physical guide material, along which a signal is propagated. Examples include wire pairs, coaxial cable, and optical fibers.

e. Unguided media is defined as a transmission path that does not employ physical guide material. Examples include satellite, microwave and laser/maser free-space paths.

f. Circuit/trunk/link definitions are dependent upon usage and termination points and are formalized in FED-STD-1037 and BELCORE standards.

g. Sensitive unclassified information is any information whose loss, misuse, or unauthorized access to, or modification of, might adversely affect U.S. national interest, the conduct of DOD programs, or the privacy of DOD personnel.

h. Unclassified information is any information that need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste, or abuse.

3. Policy

a. Per reference (a), information, information-based processes, and information systems, such as Command, Control, Communications, and Computer (C4) systems, weapon systems, and infrastructure systems, etc., used by U.S. military forces shall be protected relative to the value of the information contained therein and the risks associated with its compromise or loss. For the USUSEUCOM, all links/trunks shall be bulk encrypted to the highest data rate possible. Bulk encryption shall be routinely applied to future fixed plant and strategic transmission systems within the European theater and for those trunks that originate from the East coast of the continental United States. Bulk encryption application shall be considered whenever existing systems are expanded, modified or upgraded. Bulk encryption hardware design objectives shall not be compromised in any way to meet cost guidelines.

b. Except for emergencies, sensitive unclassified information transmitted electronically on all military multichannel radio systems and DCS satellite; including tactical, non-tactical, government-owned/commercial leased, or acquired domestic multichannel radio and satellite systems or services, shall be encrypted by means of on-line encryption devices approved by the National Institute of Standards and Technology (NIST) or NSA. If any unencrypted sensitive unclassified circuit exists in a data stream, bulk encryption is mandatory. A risk assessment should be made by the O&M command and if acceptable, a waiver should be forwarded in accordance with paragraph 6.

c. Except for emergencies, sensitive unclassified information that employs guided media (i.e., fiber optic or metallic cable) shall be link or bulk encrypted by means of on-line encryption devices approved by NIST or NSA if the entire run is NOT:

(1) Completely within the physical confines of U.S. government controlled property.

(2) Encrypted for that portion of the media run outside the physical confines of U.S. government control.

(3) Completely enclosed within an NSA PDS Category 3a or better protective distribution system (PDS) as approved by the individual services or joint commands.

(4) Exempted in writing by ECJ6-I or his designated representative.

b. Bulk encryption implementation for existing systems and links that are not being expanded, modified or upgraded is required if any existing and potential links are not link encrypted. Planning and budgeting for such encryption is the responsibility of the Service with O&M responsibility. Exemption procedures for these encryption requirements are covered in paragraph 7.

4. Waiver Authority

a. ECJ6-I

(1) T-1 and above.

(2) All inter country/West Coast/Alaska circuits/trunks/links.

b. USFK, USFJ and ALCOM/ECJ6s - Intra-country circuits/links below T-1 data rate.

5. Waiver Procedures

a. Waivers shall be submitted to ECJ6-I no later than 90 days prior to activation of circuits/trunks/links.

b. Waiver requests shall be forwarded in writing from the appropriate O&M command to the subunified command or Service. A waiver example is provided as an annex to this appendix.

(1) T-1 and above. The subunified command shall concur or nonconcur waiver request to ECJ6-I and provide copies to the appropriate Defense Information Systems Agency (DISA) Field Office (FO) and DISA-Europe (DISA-EUR)/PC5.

(2) Intra-country circuits/links below T-1 data rate. The subunified command shall review, evaluate and approve waiver request. Copies of locally approved waivers shall be forwarded to USEUCOM ECJ61 and DISA-EUR.

c. Depending on the waiver authority, ECJ6-I or the subunified command may verbally grant a 120-day implementation delay immediately upon the first application. This approval shall be followed up in writing. The circuit/trunk/link may be brought on-line and allowed to pass unclassified traffic during this implementation delay at the discretion of the O&M commander. A second and third implementation delay may be granted in writing. No more than three implementation delays may be granted during the life of a circuit/trunk/link.

6. Exemptions. Exemptions to this policy may only be granted in writing by ECJ6-I at the request of the O&M commander with a recommendation by DISA-EUR under the following conditions:

a. The circuit/trunk/link has a demonstrable life-span of less than three calendar years from the date of application for exemption.

b. The circuit/trunk/link terminates with a non-U.S., non-allied private organization.

c. The circuit/trunk/link provides only special purpose, single function communications (e.g., fire and intrusion alarms, light and siren controls, crash net indicators, etc.)

d. The circuit/trunk/link exhibits special technical considerations that render it incompatible with existing approved encryption systems (e.g., interswitch controls, non-standard format audio and video links, etc.).

e. Other conditions as approved by ECJ6-I with the advice and consent of DISA-EUR.

7. Policy For Bypassing Encryption Devices

a. Technical control facilities should verify whether the bulk encryption device is defective or the characteristics of the transmission path is causing the problem.

b. If alternate encrypted paths are not available, the technical control facilities may request permission to put cryptographic devices in bypass mode to restore the circuit/trunk/link to service from the DISA-EUR Regional Control Center (RCC) through the servicing facility control office (FCO). Do not put cryptographic devices in bypass without permission from the RCC. Once the RCC receives the request, DISA-EUR shall validate the waiver and authorize a maximum of 48 hours that the circuit/trunk/link be put in the bypass mode.

c. If the cryptographic devices cannot be returned to service after 48 hours, service shall be rerouted to an encrypted path, if available or applicable. To continue bypass mode, waiver approval is required from ECJ6-I using paragraph 6 procedures.

d. If cryptographic devices cannot be restored and the circuit/trunk/link is deemed necessary to be shut down by the O&M command and RCC, a request shall be forwarded, with validation from DISA-EUR, to HQ ECJ6-I for approval or disapproval. No action shall be taken to shut down the circuit until advised by the RCC.

8. Cryptographic Equipment. Transmission links supporting sensitive unclassified information shall be bulk encrypted using products validated by the National Institute of Standards and Technology (NIST) as meeting the criteria of applicable federal information processing standards or by NSA endorsed products. All classified information must be encrypted by NSA Type 1 products.

9. Risk Assessment. When requesting a bulk encryption waiver or bypass, a risk assessment must be done at the O&M command. At a minimum, review the threat and identify the priority users of the link, if applicable. This requirement is on the waiver example.

APPENDIX F – BULK ENCRYPTION POLICY

Annex A – Bulk Encryption Waiver Example

MEMORANDUM FOR Headquarters, United States European Command, ATTN: ECJ6,
Unit 30400, Box 1000, APO AE 09128

THRU Headquarters, United States European Command, ATTN: ECJ6-I/ECJ6-S,
Unit 30400, Box 1000, APO AE 09128

SUBJECT: Bulk Encryption Waiver/Bypass Request

1. Request waiver of USEUCOM policy for bulk encrypting terrestrial transmission links.

   a. Description of link/trunk

      (1) CCSD
      (2) End locations
      (3) Data rate
      (4) Type of transmission media
      (5) Type of traffic
      (6) Current status of Link/Trunk

   b. Circuit POC

      (1) Name, Rank
      (2) Organization
      (3) DSN telephone numbers, AUTODIN message address and e-mail

   c. Reason for waiver/bypass request

   d. Risk Assessment

   e. Proposed timeline for implementing bulk encryption

   f. Special Considerations

2. POC for this request is _____, DSN _____, e-mail _____

SIGNATURE BLOCK

(This page intentionally left blank)

DIRECTIVE NUMBER 25-5

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

Glossary of Terms

ADP - Automated Data Process
AIS - Automated Information System
AOR - Area of Responsibility
C2 - Command and Control
C4 - Command, Control, Communications, and Computers
C4I - Command, Control, Communications, Computers, and Intelligence
CAT - Crisis Action Team
CNA – Computer Network Attack
CND – Computer Network Defense
DAA – Designated Approving Authority
DEFCON - Defense Condition
DISA-EUR - Defense Information Systems Agency - Europe
EW - Electronic Warfare
FAX - Facsimile Machine
GCCS - Global Command and Control System
GOSC - Global Operation Support Cell
IAW - In Accordance With
IDS – Intrusion Detection System
INFOCONS - Information Operations Condition
IO - Information Operations
IOC – Information Operations Cell
IP - Internet Protocol
IW - Information Warfare
I&W - Indications and Warnings
ISSM - Information System Security Manager
ISSO - Information System Security Officer
JAC - Joint Analysis Center Europe
JIDS - Joint Intrusion Detection System
JTF- Joint Task Force
LAN - Local Area Network
NIPRNET - Nonsecure internet protocol routing network
OPSEC - Operations Security
PA - Public Affairs
PASS - Europe ADP Server System
PSYOP - Psychological Operations
ROSC- Regional Information System Security Cell
SA - System Administrator
SCI - Sensitive Compartmented Information
SIPRNET - Secure Internet Protocol Routing Network
SITREPS - Situation Updates
SMG - Secure Mail Guards
THREATCON - Threat Condition

WWW - World Wide Web

LIST OF EFFECTIVE PAGES (LOEP)

Page(s), Annex, Appendix	Change	Date of Change
i - v	Orig	01 Mar 99
1 - 8	Orig	01 Mar 99
Appendix A	Orig	01 Mar 99
Appendix A, Annex A	Orig	01 Mar 99
Appendix B	Orig	01 Mar 99
Appendix B, Annex A	Orig	01 Mar 99
Appendix B, Annex B	Orig	01 Mar 99
Appendix C	Orig	01 Mar 99
Appendix C, Annex A	Orig	01 Mar 99
Appendix C, Annex B	Orig	01 Mar 99
Appendix C, Annex C	Orig	01 Mar 99
Appendix C, Annex D	Orig	01 Mar 99
Appendix D	Orig	01 Mar 99
Appendix D, Annex A	Orig	01 Mar 99
Appendix D, Annex B	Orig	01 Mar 99
Appendix E	Orig	01 Mar 99
Appendix F	Orig	01 Mar 99
Appendix F, Annex A	Orig	01 Mar 99

(This page intentionally left blank)

HEADQUARTERS
UNITED STATES
EUROPEAN COMMAND
STUTTGART, GERMANY

USEUCOM DIRECTIVE 25-5

INFORMATION ASSURANCE

01 March 1999

ECJ6